VVSG Security Requirements: Next Steps

Presentation for the
Technical Guidelines Development Committee (TGDC)

Nelson Hastings

September 29, 2005
National Institute of Standards and Technology

Overview

- Approach and Methodology
- Recap
- Current Activities
- January 2006 Activities
- April 2006 and Beyond Activities
- Discussion

Approach and Methodology

- Most resolutions affect development of the security requirements

- 12-05: Voter Verifiability I
- 14-05: Commercial Off The Shelf (COTS) Software
- 15-05: Software Distribution
- 16-05: Setup Validation
- 17-05: Testing
- 18-05: Documentation
- 21-05: Multiple Representation of Ballots
- 22-05: Federal Standards
- 23-05: Common Ballot Format Specification
- 35-05: Wireless
- 39-05: VVPAT

Approach and Methodology

- Requirements developed based on
  - Voting System Standard (VSS) 2002
  - IEEE P1583
  - Voluntary Voting System Guideline (VVSG)
  - New requirements will be developed as needed
  - Use the results from threat analysis work

Approach and Methodology

- Consolidate general security requirements (e.g. Cryptography) in a comprehensive security section
- Specific security requirements added as need to other sections
  - Security requirements for Casting section
  - Security requirements for Counting and Reporting section

Recap

- Software Distribution Requirements
  - Addresses Res. 15-05: Software Distribution
  - Cryptographic aspects to be moved into a general cryptography section
- Setup Validation Requirements
  - Addresses Res. 16-05: Setup Validation
  - Integrated with a comprehensive System Integrity Management section

Recap

- Wireless Requirements
  - Addresses Res. 35-05: Wireless
  - Provide a comprehensive Communications Section that includes wireless, wired, etc.
- Independent Dual Verification (IDV)
  - Addresses Res. 12-05: Voter Verifiability I
  - Cover Voter Verified Paper Audit Trail (VVPAT)
  - Details provided in another presentation

Current Activities

- Threat Analysis Work
  - Address the plausibility of key threats such as Trojan horses within software
  - Threat analysis workshop to be held on October 7, 2005
  - Results will feed into the development of security requirements

Current Activities

- Open Ended Testing
  - Researching and developing a white paper to address Res. 17-05: Testing
  - Completed by January 2006
  - Results to be incorporated into the Testing Standard section

Current Activities

- Security issues related to core requirements
  - Create an access control role model
  - Security-related documentation
  - Security requirements for the transmission of results

January 2006 Activities

- Starting with “core” security requirements
- Research and develop sections on:
  - Cryptography
  - Software Distribution and Installation
  - Access Control
  - System Auditing and Event Logging

April 2006 and Beyond Activities

- Research and develop sections on:
  - Physical Security - April 2006
  - Communications - April 2006
  - System Integrity Management - July 2006
  - Hardware Security - July 2006
  - Independent Dual Verification (IDV) Profile - October 2006
  - Threat Analysis Appendix - January 2007

Discussion